Abschlussprüfung Winter 2025/26
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).
Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=	100 – 92 Punkte	Note 2	= unter	92 – 81 Punkte
Note 3	= unter	81 – 67 Punkte	Note 4	= unter	67 – 50 Punkte
Note 5	= unter	50 – 30 Punkte	Note 6	= unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2025 – Alle Rechte vorbehalten!

1. Aufgabe (26 Punke)

aa) 6 Punkte

Router	Interface	IP-Adresse des Interface	Anzahl nutzbarer IP-Adressen
Zentrale	eth1 - LAN	10.63.255.254	2^22 – 2 bzw. 4.194.302
Zentrale	eth2 - DMZ	192.168.199.254	2^8 – 2 bzw. 254
Reisebüro	eth1 - LAN	192.168.51.254	2^9 – 2 bzw. 510

ab) 6 Punkte

Router Zentrale			
Netzwerk-ID	CIDR	Schnittstelle	Next-Hop
10.0.0.0	/10	Eth1	---
192.168.199.0	/24	Eth2	---
31.101.17.40	/30	Eth0	---
172.16.10.0	/30	Tun0	---
172.16.20.0	/30	Tun1	---
192.168.23.0	/24	---	172.16.10.2
192.168.50.0	/23	---	172.16.20.2
0.0.0.0	/0	---	31.101.17.42

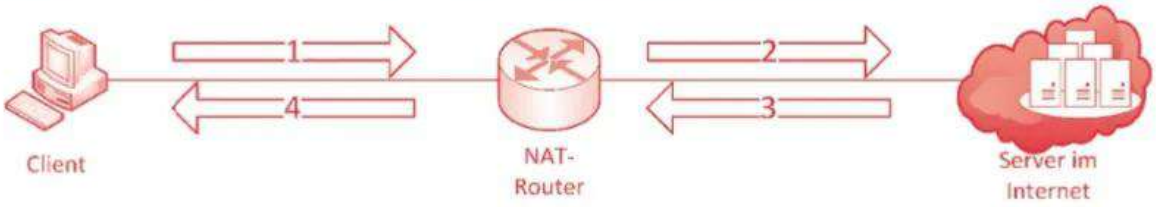
ba) 2 Punkte

Die Pakete werden mit einer privaten Absender-Adresse losgeschickt, diese werden im Internet nicht geroutet. (Würden Sie „einfach so" ins Internet geleitet werden, wäre es für den Server im Internet unmöglich, eine Antwort an den Absender-PC zurückzusenden.)

bb) 6 Punkte

Abschnitt 1	
Source	Destination
10.0.0.1:45123	12.7.51.9:443
10.0.0.2:45123	12.7.51.9:443

Abschnitt 2	
Source	Destination
31.101.17.41:45123 siehe Anmerkung 1	12.7.51.9:443
31.101.17.41:45124 siehe Anmerkung 1	12.7.51.9:443



Abschnitt 4	
Source	Destination
12.7.51.9:443	10.0.0.1:45123
12.7.51.9:443	10.0.0.2:45123

Abschnitt 3	
Source	Destination
12.7.51.9:443	31.101.17.41:45123 siehe Anmerkung 2
12.7.51.9.443	31.101.17.41:45124 siehe Anmerkung 2

Anmerkung 1: Andere, beliebige Ports im Bereich von 1.024 bis 65.535 sind auch möglich, sofern für beide NAT/PAT-Vorgänge unterschiedliche Ports gewählt werden.

Anmerkung 2: Die hier angegebenen Ports müssen denen in Abschnitt 2 entsprechen.

bc) 3 Punkte

Durch TLS wird nur der Nutzdatenanteil geschützt. Die Header-Felder, in denen die Quell-IP/Port und Ziel-IP/Port transportiert werden, können vom NAT-Router verändert werden, ohne dass dadurch die Verschlüsselung aufgebrochen wird.

bd) 3 Punkte

Portforwarding (Destination NAT) übersetzt anhand des Zielports, z. B. 80 für HTTP, die öffentliche Ziel-IP in die gewünschte interne, private IP. Damit kann z. B. ein Webserver im privaten Netz (hier DMZ) von außen erreichbar gemacht werden.

2. Aufgabe (26 Punke)

aa) 2 Punkte
Einrichtung eines Site-to-Site-VPN. Das VPN wird auf beiden Seiten auf einem VPN-Gateway oder dem Router oder der Firewall eingerichtet, welche(s) den sicheren Tunnel für die Kommunikation zwischen Endgeräten im internen Netzwerk aufbaut.

ab) 2 Punkte
Remote Access VPN/End-to-site VPN/Roadwarrior:
Das VPN muss im Firmennetz auf einem VPN-Gateway/Router/Firewall eingerichtet werden und bei Busfahrer oder Reiseleitung auf dem jeweiligen Endgerät (Smartphone/Tablet/Laptop).

b) 4 Punkte
Vertraulichkeit: Die Information kann nur von befugten Instanzen eingesehen werden.
Integrität: Daten werden unverändert zwischen den Instanzen übertragen.
Authentizität: Die Identität beider Instanzen ist sichergestellt.

c) 6 Punkte
Alle möglichen Ursachen, die zu diesem Problem führen können, sind als korrekte Lösung zu werten.

Beispiele:
Fehlerhafte Authentifizierungsdaten (z. B. Passwort falsch)
VPN-Client nicht richtig installiert oder konfiguriert
ISP blockiert VPN-Verbindungen
VPN-Gateway ist für diesen Benutzer nicht konfiguriert
MTU zu hoch, Paket wird nochmal fragmentiert und deswegen verworfen (VPN-Header kann nicht ergänzt werden)

Fehlersuche:
Netzwerkverbindung: Überprüfen, ob der Nutzer eine funktionierende Internetverbindung hat.
VPN-Konfiguration: Überprüfen der VPN-Einstellungen (z. B. Serveradresse, Authentifizierungsdaten).
Firewall oder Antivirensoftware: Überprüfen, ob eine lokale Firewall oder Antivirensoftware die VPN-Verbindung blockiert.
Protokoll-Einstellungen: Sicherstellen, dass das richtige VPN-Protokoll (z. B. IKEv2 oder OpenVPN) verwendet wird.
Nutzerrechte: Überprüfen, ob der Nutzer die notwendigen Rechte für den VPN-Zugang hat.

da) 4 Punkte
Verbesserung der Passwortsicherheit:
- Passwörter müssen eine Mindestanzahl an Zeichen haben.
- Passwörter sollten (Groß- und Kleinbuchstaben,) Zahlen und Sonderzeichen enthalten.
- User sollten gezwungen werden, Passwörter zu ändern, wenn Leaks bekannt werden.
- Passwörter dürfen keine bekannten Worte enthalten.
- Passwörter dürfen keine Bestandteile von Vor- oder Nachnamen enthalten.
- Passwörter dürfen keine „trivialen" Zeichenfolgen enthalten.

db) 4 Punkte
- Besitz: Nutzung von etwas, das der Nutzer besitzt (z. B. Smartphone-Token).
- Biometrisches Merkmal: Fingerabdruck- oder Gesichtserkennungstechnologien.
- Fähigkeit: Lösen eines CAPTCHAS.
- Authentifizierung durch Dritte: Identifizierung durch eine weitere Instanz, Personenkontrolle.

e) 4 Punkte

Angriffsmethode	Erläuterung
Phishing	Der Versuch, sich als vertrauenswürdiger Kommunikationspartner auszugeben, mit dem Ziel, an vertrauliche Daten des Benutzers zu gelangen.
Trojaner	Tarnt sich als legitime Software um Zugriff auf das System eines Benutzers zu erlangen.
Virus	Schadsoftware, die unbemerkt auf ein Rechnersystem eingeschleust wird und sich repliziert.

Andere sinnvolle Lösungen sind möglich.

3. Aufgabe (24 Punkte)

aa) 4 Punkte
- Mehr Sicherheit, da logische Trennung der Netzwerke
- Mehr Flexibilität, da neue Netzsegmente leicht erzeugt werden können
- Weniger Hardware, da mehrere Netzwerke auf einem Switch/Kabel laufen
- Weniger Kosten, da weniger Hardware benötigt wird
- Weniger Verkabelung, da mehrere Netzwerke auf einem Switch/Kabel laufen
- u. a.

ab) 5 Punkte (je 1 Punkt für die Zeilen G0/10, G0/22, G0/23, 2 Punkte für die Zeile G0/24)

Interface	VLAN-Nr	Switchportmodus
G0/1	233	untagged
G0/2	233	untagged
G0/10	232	untagged
G0/22	231	untagged
G0/23	231	untagged
G0/24	231,232,233	tagged

ba) 3 Punkte
Ermöglicht es, Datenverkehr zwischen mehreren VLANs über einen einzigen Routerport zu routen. Jedes VLAN besitzt dabei ein eigenes Subinterface (virtuelles Interface) auf dem Router, für das eine spezifische IP-Adresse als Gateway für das zugehörige Subnetz konfiguriert ist.

bb) 3 Punkte
Fehlerbeschreibung:
IP-Adresse für das Gateway des Netzes der festen PCs (VLAN 231) ist falsch, die .61 liegt nicht im angegebenen Netzbereich.

Konkreter Lösungsvorschlag:
Interface Gig0/0.231 mit einer IP-Adresse aus dem Bereich 192.168.23.1 bis .6 und SNM 255.255.255.248 konfigurieren

bc) 3 Punkte
Ermöglicht dem Router VLAN-Tagging, sodass Datenpakete unterschiedlicher VLANs über eine physische Schnittstelle geschickt werden können und die VLAN-ID ausgewertet werden kann.

c) 6 Punkte
- Priorisierung des Netzwerkverkehrs (QoS) durch Trennung des Datenverkehrs von der Telefonie möglich
- Erhöhte Sicherheit, da Ports für VoIP-Telefone von Datennetz getrennt werden können
- Schutz vor Angriffen (z. B. DoS oder Spoofing), da vom Datennetz getrennt
- Einfachere Fehlerdiagnose, da VoIP-Verkehr isoliert
- Bessere Skalierbarkeit, da VoIP-Netz an neue Telefone einfach angepasst werden kann
- u. a.

4. Aufgabe (24 Punkte)

a) 3 Punkte
Antwort:
365 Tage x 24 Stunden pro Tag = 8.760 Stunden. Hiervon 1 % sind 87,6 Stunden.

ba) 3 Punkte
Antwort: Es kommen nur Satellit oder FTTH in Betracht mit einer Verfügbarkeit von 99 %
1 – (0,01 * 0,01) = 0,9999 (99,99 %)

bb) 2 Punkte
Nachteil bei Shared-Medium: Mehrere Endpunkte (= Kunden) teilen sich die verfügbare Bandbreite (= Gesamtkapazität) im jeweiligen Netzsegment des Providers. Die tatsächlich zur Verfügung stehende Bandbreite ist davon abhängig, wie viel Bandbreite im Netzsegment von den anderen Kunden im selben Segment genutzt wird.

bc) 4 Punkte
15 GiB * 1.024 Byte / KiB * 1024 KiB / MiB * 1024 MiB / GiB
= 15 * 1.073.741.824 Byte
= 16.106.127.360 Byte

16.106.127.360 Byte * 8 bit/Byte
= 128.849.018.880 bit

128.849.018.880 * 1,1 (Overhead)
= 141.733.920.768 bit

141.733.920.768 bit / 250.000.000 bit/s
= 566,94 Sekunden

9 Minuten 27 Sekunden

Andere Darstellungen des Rechenwegs sind möglich.

bd) 2 Punkte
Öffentliche IPv4-Adresse kostenpflichtig bestellen
IPv6 zum Aufbau des Tunnelprotokolls verwenden

ca) 4 Punkte
Der Switch-Port ist als Uplink eingerichtet. Der komplette Netzwerkverkehr der Abteilung geht gebündelt über diesen Port.

Der Switch-Port steht auf Monitoring. Der komplette Netzwerkverkehr wird zu Diagnosezwecken an diesen Port geleitet.

An diesem Port wird ein „Man in the Middle"-Angriff durchgeführt. Z. B. durch ARP-Spoofing wird erhöhter Netzwerkverkehr über den angeschlossenen Rechner umgeleitet.

Weitere Lösungen sind möglich.

cb) 6 Punkte (je 2 Punkte für Ursache und 1 Punkt für Fehlerbeseitigung)
Es werden zwei Ursachen und Fehlerbeseitigungen erwartet. Die folgende Auflistung ist beispielhaft zu verstehen, andere Ursachen und Fehlerbeseitigungen sind, sofern korrekt, ebenfalls zu werten.

Ursache: (übernommene Konfiguration falsch)
Die SFP-Ports sind mit den letzten Kupfer-Ports des Switches shared. Somit liegt die Konfiguration auf einen falschen Port.
Fehlerbeseitigung:
Konfiguration der Glasfaserschnittstelle auf den entsprechen Port durchführen.

Ursache: (übernommene Konfiguration falsch)
Die SFP-Ports kommen nach den Kupfer-Ports. Somit liegt die Konfiguration nun auf einen höheren falschen Port.
Fehlerbeseitigung:
Konfiguration der Glasfaserschnittstelle auf den entsprechen Port durchführen.

Ursache: (Falsches SFP-Modul verbaut)
Das neue SFP-Modul hat eine andere Wellenlänge. Bei unterschiedlichen Wellenlängen kommt keine Verbindung zustande.
Fehlerbeseitigung:
Auf beiden Seiten der Glasfaserverbindung die Wellenlänge der SFP-Module prüfen. Und auf beiden Seiten der Glasfaserverbindung SFP-Module mit gleicher Wellenlänge verwenden.

Ursache: (Sende-/Empfangsrichtung getauscht)
Beim Einstecken der Glasfasern wurden Sende- und Empfangsrichtung getauscht. Keine Kommunikation möglich, da nicht auf einer Faser Sender und Empfänger liegen.
Fehlerbeseitigung:
Auf einer Seite der Glasfaserverbindung die Fasern/Stecker tauschen.

Ursache: (optischer Fehler)
Die optischen Kontakte sind am SFP-Modul oder/und am Glasfaserstecker verschmutzt.
Fehlerbeseitigung:
Optische Kontakte reinigen.

Ursache: (elektrischer Fehler des SFP-Moduls)
Schlechter Kontakt des SFP-Moduls im Steckplatz oder SFP-Modul defekt
Fehlerbeseitigung:
Elektrische Kontakte säubern. Evtl. mehrmaliges ein- und aufstecken des SFP-Moduls.
Wenn neues SFP-Modul defekt, dann altes SFP-Modul testweise einsetzen.